Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2724

(11/2013)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

Réseaux de prochaine génération – Sécurité

Cadre pour la prise en charge d'OAuth et d'OpenID dans les réseaux de prochaine génération

Recommandation UIT-T Y.2724

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Améliorations concernant les réseaux de prochaine génération	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Réseaux de transmission par paquets	Y.2600–Y.2699
Sécurité	**Y.2700–Y.2799**
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
RÉSEAUX FUTURS	Y.3000–Y.3499
INFORMATIQUE EN NUAGE	Y.3500–Y.3999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Y.2724

Cadre pour la prise en charge d'OAuth et d'OpenID dans les réseaux de prochaine génération

Résumé

La Recommandation UIT-T Y.2724 décrit un cadre pour la prise en charge et l'utilisation du protocole d'autorisation ouvert de l'IETF (OAuth) et du protocole OpenID dans le contexte des réseaux de prochaine génération (NGN). Ces deux protocoles ont été définis pour être utilisés d'une manière générale sur le web dans le monde.

Les exigences plus rigoureuses applicables aux réseaux NGN en matière de sécurité et de gestion d'identité supposent l'application de restrictions précises aux protocoles susmentionnés. Cette Recommandation explique comment appliquer ces protocoles aux réseaux NGN et donne des lignes directrices de haut niveau pour leur utilisation.

La Recommandation UIT-T Y.2723 associée ("Prise en charge d'OAuth dans les réseaux de prochaine génération") contient un ensemble détaillé de profils NGN.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T Y.2724	2013-11-15	13	11.1002/1000/11914

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T Y.2724

Cadre pour la prise en charge d'OAuth et d'OpenID dans les réseaux de prochaine génération

1 Domaine d'application

La présente Recommandation décrit un cadre pour la prise en charge et l'utilisation des protocoles OAuth et OpenID par les réseaux NGN. Elle porte sur les domaines suivants:

- Cadre fonctionnel pour la prise en charge des protocoles OAuth et OpenID dans les réseaux NGN.
- Prescriptions applicables à la prise en charge des protocoles OAuth et OpenID dans les réseaux NGN.
- Cas d'utilisation des protocoles OAuth et OpenID (présentés dans l'Appendice I).

NOTE – Les responsables de la mise en œuvre et les opérateurs utilisant la technologie décrite doivent se conformer aux législations, réglementations et politiques nationales ou régionales applicables.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T Y.2012] Recommandation UIT-T Y.2012 (2010), *Prescriptions et architecture fonctionnelles du réseau de prochaine génération.*

[UIT-T Y.2720] Recommandation UIT-T Y.2720 (2009), *Cadre de gestion d'identité des réseaux NGN.*

[ITU-T Y.2722] Recommandation UIT-T Y.2722 (2011), *Mécanismes de gestion d'identité dans les réseaux de prochaine génération.*

[IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 Authorization Framework* <http://tools.ietf.org/html/rfc6749>

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 jeton d'accès [IETF RFC 6749]: justificatif utilisé pour accéder à une ressource protégée. Un jeton d'accès est une chaîne représentant une autorisation délivrée au client. Cette chaîne est généralement opaque pour le client. Les jetons représentent des types et durées d'accès spécifiques accordés par le propriétaire de ressources et appliqués par le serveur de ressources et le serveur d'autorisation.

3.1.2 authentification (d'entité) [b-UIT-T X.1252]: processus utilisé pour obtenir une confiance suffisante dans le lien entre l'entité et l'identité présentée.

NOTE – Dans un contexte de gestion d'identité (IdM), le terme authentification désigne l'authentification d'entité.

3.1.3 autorisation [b-UIT-T X.800]: attribution de droits comprenant la permission d'accès sur la base de droits d'accès.

3.1.4 serveur d'autorisation [IETF RFC 6749]: serveur délivrant des jetons d'accès au client une fois menées à bien l'authentification du propriétaire de ressources et l'obtention de l'autorisation.

3.1.5 client [IETF RFC 6749]: application soumettant des demandes de ressource protégée pour le compte du propriétaire de ressources et avec son autorisation. Le terme "client" n'implique aucune caractéristique particulière pour la mise en œuvre (par exemple l'application peut être exécutée aussi bien sur un serveur, que sur un ordinateur de bureau ou sur d'autres dispositifs).

3.1.6 entité [b-UIT-T X.1252]: élément qui a une existence séparée et distincte et peut être identifié dans un contexte.

NOTE – Une entité peut être une personne physique, un animal, une personne morale, une organisation, une chose active ou passive, un dispositif, une application logicielle, un service, etc., ou un groupe de ces entités. Dans le contexte des télécommunications, il peut s'agir de points d'accès, d'abonnés, d'utilisateurs, d'éléments de réseau, de réseaux, d'applications logicielles, de services et de dispositifs, d'interfaces, etc.

3.1.7 identificateur [b-UIT-T X.1252]: un ou plusieurs attributs utilisés pour identifier une entité dans un contexte.

NOTE – Dans le contexte des NGN tel qu'il est défini dans [b-UIT-T Y.2091], un identificateur est une suite de chiffres, de caractères, de symboles ou de toute autre forme de données, utilisée pour identifier un ou plusieurs abonnés, utilisateurs, éléments de réseau, fonctions, entités de réseau fournissant des services ou des applications, ou d'autres entités (par exemple des objets physiques ou logiques).

3.1.8 fournisseur d'identité (IdP) [b-UIT-T X.1252]: voir fournisseur de service d'identité (IdSP).

3.1.9 fournisseur de service d'identité (IdSP) [b-UIT-T X.1252]: entité qui vérifie, tient à jour, gère et peut créer et attribuer des informations d'identité d'autres entités.

3.1.10 jeton d'actualisation [IETF RFC 6749]: jeton délivré au client par le serveur d'autorisation et utilisé pour obtenir un nouveau jeton d'accès lorsque le jeton d'accès existant n'est plus valide ou arrive à expiration, ou pour obtenir des jetons d'accès supplémentaires ouvrant des droits identiques ou plus limités (les jetons d'accès peuvent avoir une durée de vie plus courte et contenir moins de permissions que ce qu'autorise le propriétaire de ressources). L'émission d'un jeton d'actualisation est facultative et dépend du serveur d'autorisation. Si le serveur d'autorisation délivre un jeton d'actualisation, celui-ci est émis en même temps que le jeton d'accès.

3.1.11 propriétaire de ressources [IETF RFC 6749]: entité capable d'octroyer l'accès à une ressource protégée. Lorsque le propriétaire de ressources est une personne, il est appelé utilisateur final.

3.1.12 serveur de ressources [IETF RFC 6749]: serveur hébergeant les ressources protégées, capable d'accepter les demandes de ressource protégée utilisant des jetons d'accès et de répondre à ces demandes.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation emploie les abréviations et les acronymes suivants:

AKA authentification et accord de clé (*authentication and key agreement*)

ANI interface application-réseau (*application-to-network interface*)

FE entité fonctionnelle (*functional entity*)

GBA architecture d'amorçage générique (*generic bootstrapping archirtecture*)

IdM gestion d'identité (*identity management*)

IdP fournisseur d'identité (*identity provider*)

IdSP fournisseur de service d'identité (*identity service provider*)

IMPI identité privée multimédia IP (*IP multimedia private identity)*

IMSI identité internationale d'abonné mobile (*international mobile subscriber identity*)

NGN réseau de prochaine génération (*next generation network*)

SAML langage de balisage d'assertion de sécurité (*security assertion markup language*)

SNI interface service-réseau (*service network interface*)

UNI interface utilisateur-réseau (*user network interface*)

5 Conventions

Dans la présente Recommandation:

L'expression "il est obligatoire" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

L'expression "il est recommandé" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "il est interdit" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

L'expression "peut, à titre d'option" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

Dans le corps de la présente Recommandation et dans ses annexes, on trouve parfois les expressions doit, ne doit pas, devrait et peut. Celles-ci doivent respectivement être interprétées comme correspondant aux expressions il est obligatoire, il est interdit, il est recommandé et peut, à titre d'option. Lorsque ces expressions apparaissent dans un appendice ou dans des parties dans lesquelles il est expressément indiqué qu'elles sont données à titre d'information, elles doivent être interprétées comme étant dépourvues d'intention normative.

6 Cadre pour la prise en charge des protocoles OAuth et OpenID dans les réseaux NGN

Comme indiqué dans [UIT-T Y.2720], un réseau NGN est composé de plusieurs éléments fonctionnels qui fonctionnent avec des identificateurs d'entités, l'objectif étant de prendre en charge et de faciliter des services d'authentification ouverts pour d'autres fournisseurs. On pourrait prendre en charge ce type de configurations en utilisant les protocoles OpenID et OAuth comme indiqué dans la Figure 1. L'utilisation de ces deux protocoles dans les réseaux NGN est présentée dans la Figure 1.

Conformément à la spécification du protocole OpenID [b-OpenID v.2], le serveur IdP OpenID participe à tous les flux d'authentification et le protocole OAuth permet à la partie utilisatrice d'envoyer le message d'authentification directement au fournisseur NGN-IdP.

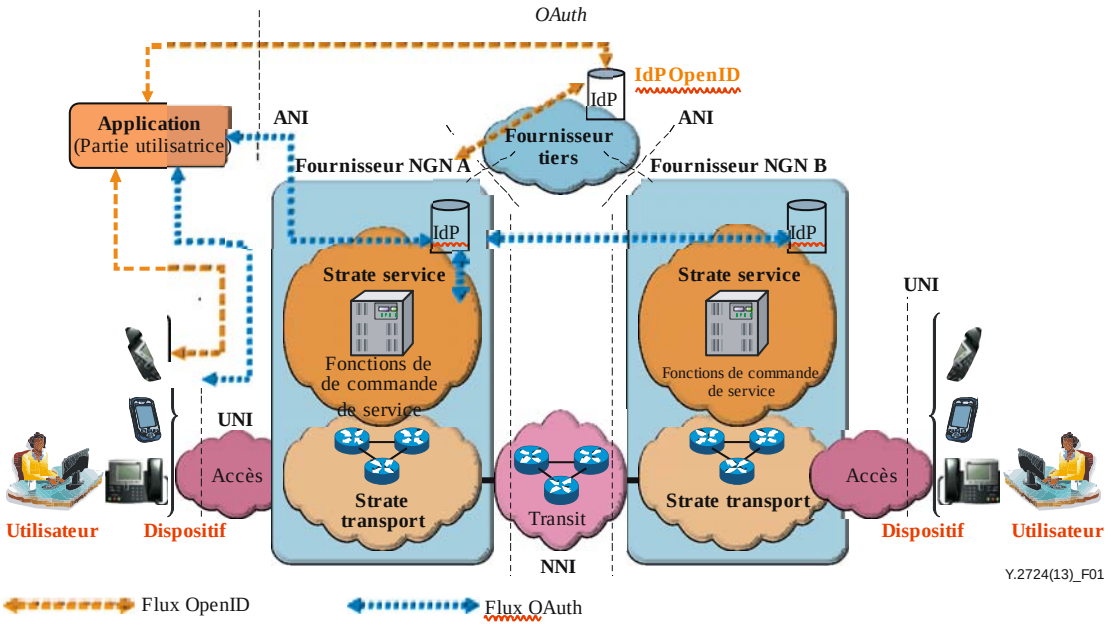

Figure 1 – Flux OpenID et OAuth pour les réseaux NGN

6.1 Modèle de référence

La Figure 1 donne un aperçu général des cadres OAuth et OpenID.

La Figure 2 décrit un modèle de référence qui permet à un réseau NGN de fournir des services d'autorisation OAuth et d'authentification OpenID. Les fournisseurs NGN peuvent utiliser les protocoles OpenID et OAuth pour offrir des services IdSP et travailler en partenariat avec des fournisseurs de contenu et d'application et/ou d'autres fournisseurs de services.

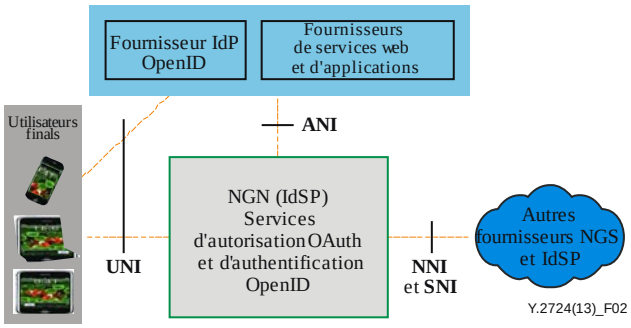

Figure 2 – Modèle de référence

6.2 Flux OAuth et OpenID

Le présent paragraphe donne une description générale des flux de messages pour les protocoles OAuth et OpenID dans les réseaux NGN.

6.2.1 Entités intervenant dans les flux d'information

Le présent paragraphe recense les entités (y compris les entités fonctionnelles décrites dans [UIT-T Y.2012]) qui participent aux flux d'information OAuth et OpenID.

6.2.2 Entités communes aux flux OAuth et OpenID

Les entités intervenant à la fois dans le flux OAuth et dans le flux OpenID sont les suivantes:

- Fonction d'utilisateur final avec la fonctionnalité d'un client web (par exemple, navigateur).
- Entité A-2: entité fonctionnelle de passerelle d'application (APL-GW-FE) [UIT-T Y.2012]. Cette entité fonctionnelle devrait être capable de prendre en charge les protocoles OAuth et/ou OpenID.

Conformément à la définition figurant dans [UIT-T Y.2012]), "l'entité APL-GW-FE constitue l'entité interfonctionnement entre différentes fonctions du NGN et tous les serveurs d'application externe et les activateurs de service". Il est donc logique de choisir l'entité A-2 pour assurer la prise en charge des protocoles OAuth et OpenID. En outre, étant donné qu'elle est connectée à l'entité S-5 – entité fonctionnelle profil d'utilisateur de service (SUP-FE) [UIT-T Y.2012], l'entité A-2 est capable de prendre en charge l'authentification fondée sur AKA, y compris l'architecture d'amorçage générique (GBA), des dispositifs d'utilisateur. Une méthode d'authentification OpenID fondée sur l'architecture GBA est définie dans [b-3GPP TS 33.220]. On trouvera dans le § 6.2.8 de [UIT-T Y.2722] une autre méthode d'authentification OpenID fondée sur AKA, analogue en certains points à celle fondée sur l'architecture GBA. Si le serveur d'autorisation OAuth et le fournisseur IdP OpenID [UIT-T Y.2722] sont tous deux mis en œuvre au niveau de l'entité A-2, ils peuvent utiliser l'authentification fondée sur AKA en interagissant avec l'entité S-5.

6.2.3 Entités propres au flux OAuth

Les entités propres au flux OAuth sont les suivantes:

- Un serveur d'application web qui accomplit un service pour un utilisateur – appelé client OAuth. Un client peut, sans en avoir l'obligation, fonctionner sur une entité NGN.
- Un serveur d'autorisation mis en œuvre dans le cadre de l'entité A-2.

  Le serveur d'autorisation procède tout d'abord à l'authentification de l'utilisateur, puis à l'autorisation de la demande du client. Si les deux procédures sont menées à bien, l'échange OAuth aboutit à la délivrance d'un jeton d'accès au client par le serveur d'autorisation. Afin de prendre en charge l'authentification fondée sur AKA, le serveur d'autorisation doit pouvoir interagir avec l'entité S-5.
- Serveur de ressources

  Le serveur de ressources accède à la demande du client lorsque celle-ci est accompagnée d'un jeton d'accès valide. Deux types de procédures permettant d'accéder à une ressource grâce à l'utilisation de jetons d'accès sont définies; les jetons support sont spécifiés dans [b-IETF RFC 6750] et l'IETF travaille actuellement à la spécification des jetons MAC. Le serveur de ressources peut être situé au même endroit que le serveur d'autorisation dans l'entité A-2.

Le niveau supérieur des flux d'information OAuth pour le cas d'utilisation relatif à un serveur web (présenté dans l'Appendice I) est décrit dans la Figure 3 et expliqué ci-après.

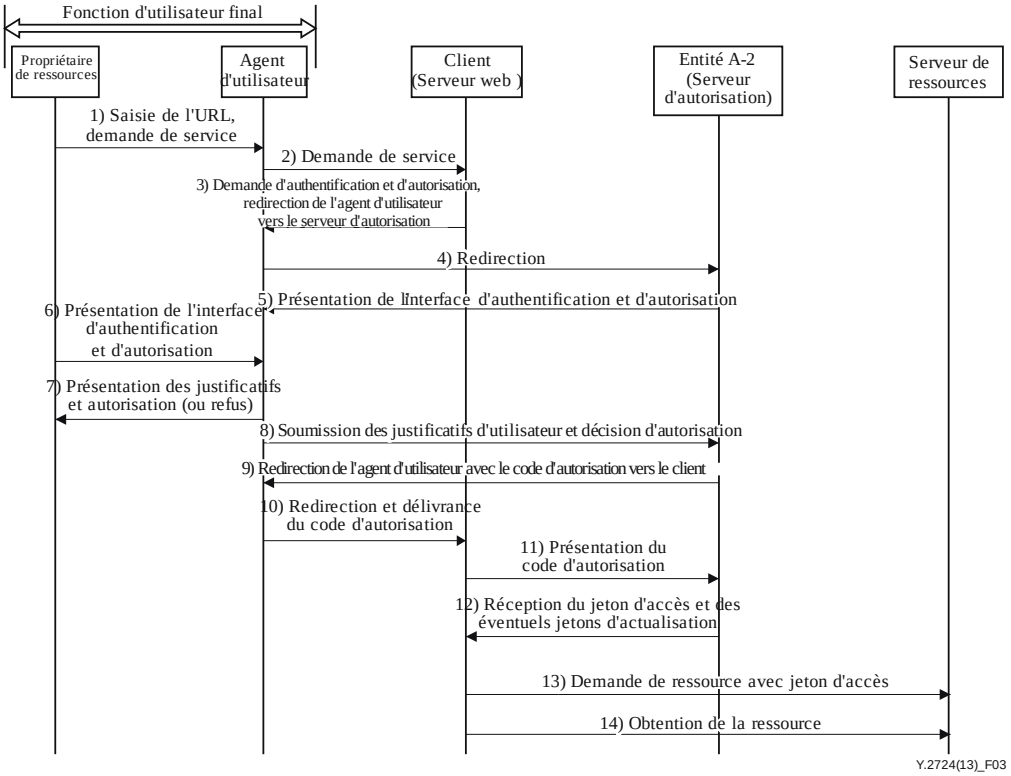

Figure 3 – Flux OAuth pour le cas d'utilisation relatif à un serveur web

1. L'utilisateur demande à l'agent d'utilisateur (par exemple le navigateur) de demander un service auprès du client.
2. L'agent d'utilisateur soumet une demande au client.
3. Le client forme une réponse et redirige l'agent d'utilisateur vers le serveur d'autorisation en vue de l'authentification et de l'autorisation de la demande du client.
4. L'agent d'utilisateur est redirigé.
5. Le serveur d'autorisation répond en fournissant à l'agent d'utilisateur l'interface d'authentification et d'autorisation.
6. L'agent d'utilisateur affiche l'interface d'authentification et d'autorisation pour l'utilisateur (propriétaire de ressources).
7. L'utilisateur fournit les justificatifs d'authentification et indique la décision d'autorisation par l'intermédiaire de l'agent d'utilisateur.
8. L'agent d'utilisateur envoie les données fournies par l'utilisateur au serveur d'autorisation.
9. Après avoir authentifié l'utilisateur et vérifié que celui-ci a autorisé la demande du client, le serveur d'autorisation redirige l'agent d'utilisateur vers le client. La réponse comprend le code d'autorisation.
10. Après avoir été redirigé, l'agent d'utilisateur fournit le code d'autorisation au client.
11. Le client envoie le code d'autorisation au serveur d'autorisation.
12. Le serveur d'autorisation répond en délivrant un jeton d'accès avec les éventuels jetons d'actualisation.
13. Le client envoie une demande au serveur de ressources et présente un jeton d'accès.
14. Le serveur de ressources fournit la ressource demandée.

6.2.4 Entités propres au flux OpenID

Les entités propres au flux OpenID sont les suivantes:

- Un serveur d'application qui s'appuie sur l'authentification faite par le fournisseur IdP OpenID.
- Un fournisseur IdP OpenID mis en œuvre dans le cadre de l'entité A-2. Afin de prendre en charge l'authentification fondée sur AKA, cette entité doit pouvoir interagir avec l'entité S-5.
- Une entité S-5, qui intervient dans l'authentification OpenID si le réseau NGN effectue une authentification fondée sur AKA de la fonction d'utilisateur final comme définie dans [UIT-T Y.2722].

Les flux d'information OpenID sont décrits dans la Figure 4 et expliqués ci-après. Le texte et la figure montrent la procédure OpenID dans le cas où le fournisseur IdP et le serveur d'application ont établi un secret partagé. Le secret permet au fournisseur IdP de signer un message contenant les résultats de l'authentification et au serveur d'application de vérifier ce message.

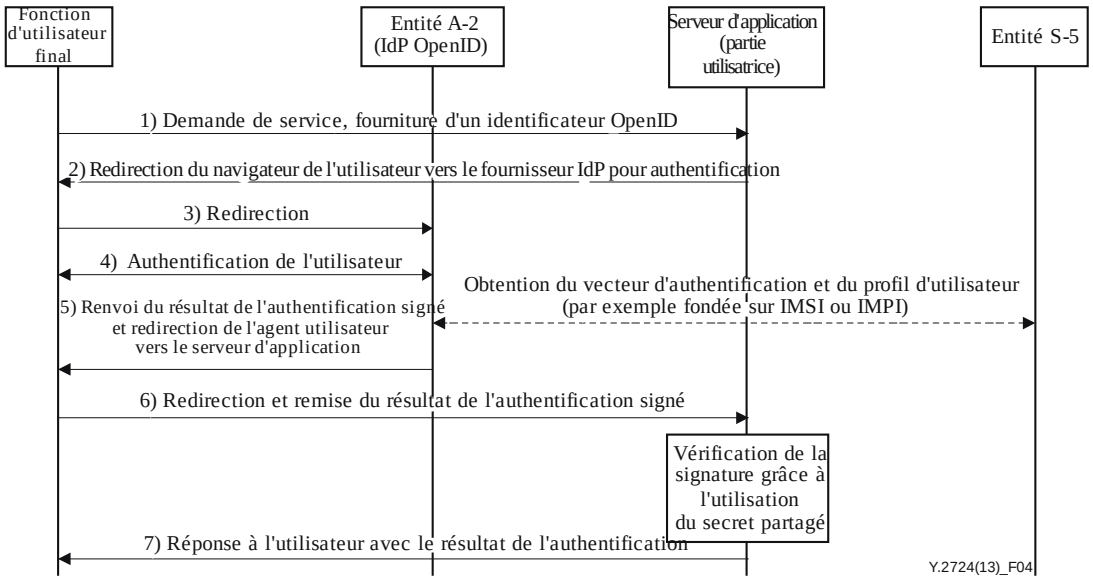

Figure 4 – Flux OpenID

1. Le navigateur de l'utilisateur envoie une demande de service à un serveur d'application; la demande contient l'identificateur OpenID de l'utilisateur.
2. A partir de l'identificateur OpenID, le serveur d'application découvre le fournisseur IdP OpenID de l'utilisateur, puis le serveur d'application redirige le navigateur de l'utilisateur vers le fournisseur IdP OpenID en vue de l'authentification.
3. Le navigateur exécute la demande de redirection.
4. Le fournisseur IdP OpenID authentifie l'utilisateur en échangeant des informations via le navigateur de l'utilisateur.
5. Si le fournisseur IdP OpenID effectue une authentification fondée sur AKA (par exemple, comme décrit dans [UIT-T Y.2722]), il doit interagir avec l'entité S-5. Ces interactions sont indiquées avec des flèches en pointillé.

6. Le fournisseur IdP OpenID redirige le navigateur de l'utilisateur vers le serveur d'application avec une réponse qui contient un message signé donnant le résultat de l'authentification.
7. Le navigateur exécute la demande de redirection et remet le message signé au serveur d'application.
8. Après avoir validé la signature et vérifié le résultat de l'authentification, le serveur d'application indique à l'utilisateur si l'authentification est réussie. Les procédures de signature et de validation sont définies dans [b-OpenID v.2].

Appendice I

Cas d'utilisation particuliers

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

I.1 Cas d'utilisation: serveur web

Description

Alice se connecte à une application installée sur un serveur web à l'adresse www.X-printphotos.example et demande l'impression de ses photographies qui sont stockées sur un serveur www.X-storephotos.example. Alice a souscrit un abonnement auprès d'un fournisseur de services NGN qui utilise un serveur d'autorisation OAuth www.X-carrier.example. L'application www.X-printphotos.example reçoit l'autorisation d'Alice d'accéder à ses photographies sans prendre connaissance de ses justificatifs d'authentification auprès de www.X-storephotos.example ou de www.X-carrier.example.

Conditions préalables

- Alice s'est enregistrée auprès de www.X-carrier.example pour permettre l'authentification.
- L'application www.X-printphotos.example a établi les justificatifs d'authentification avec le serveur d'autorisation OAuth www.X-carrier.example.
- L'application www.X-storephotos.example est capable de valider le jeton d'accès délivré par le serveur d'autorisation www.X-carrier.example.

Déroulement

Lorsque la procédure est menée à bien, l'application www.X-printphotos.example reçoit un code d'autorisation délivré par www.X-carrier.example. Ce code est lié à l'application www.X-printphotos.example et à l'adresse URL de rappel fournie par l'application. L'application www.X-printphotos.example utilise le code d'autorisation pour obtenir un jeton d'accès auprès de www.X-carrier.example. L'application www.X-carrier.example délivre un jeton d'accès après avoir authentifié l'application www.X-printphotos.example et validé le code d'autorisation qu'elle a soumis. L'application www.X-printphotos.example utilise le jeton d'accès pour obtenir l'accès aux photographies d'Alice sur www.X-storephotos.example.

NOTE – En cas d'expiration du jeton d'accès, le service www.X-printphotos.example doit répéter la procédure OAuth pour obtenir l'autorisation d'Alice d'accéder à ses photographies stockées sur www.X-storephotos.example. Autre possibilité, si Alice souhaite accorder à l'application un accès à ses ressources sur www.X-storephotos.example pour une longue durée, le serveur d'autorisation www.X-carrier.example peut délivrer les jetons longue durée correspondants. Ceux-ci peuvent être échangés contre des jetons à durée de vie réduite nécessaires pour accéder à www.X-storephotos.example.

Exigences

- Le serveur www.X-printphotos.example, qui héberge un client OAuth, doit être capable de délivrer à l'agent d'utilisateur d'Alice – un navigateur – les demandes de redirection HTTP.
- Le serveur d'autorisation www.X-carrier.example doit être en mesure d'authentifier Alice. La méthode d'authentification ne relève pas du protocole OAuth.
- L'application www.X-carrier.example doit obtenir l'autorisation d'Alice pour que www.X-printphotos.example puisse accéder à ses photos.
- L'application www.X-carrier.example peut, lorsqu'il demande l'autorisation d'Alice, lui notifier le type d'accès que www.X-printphotos.example a demandé.

- Le serveur d'autorisation www.X-carrier.example doit pouvoir authentifier l'application www.X-printphotos.example et valider le code d'autorisation avant de délivrer un jeton d'accès. L'application www.X-printphotos.example doit fournir une adresse URL de rappel au serveur d'autorisation www.X-carrier.example. (NOTE – L'adresse URL doit être enregistrée au préalable auprès de www.X-carrier.example.)
- Il est obligatoire que le serveur d'autorisation www.X-carrier.example conserve une indication du code d'autorisation associé à l'application www.X-printphotos.example et l'adresse URL de rappel fournie par l'application.
- Les jetons d'accès sont des jetons support (ils ne sont pas associés à une application spécifique, comme www.X-printphotos.example) et devraient avoir une durée de vie courte.
- Le serveur d'autorisation www.X-carrier.example doit invalider le code d'autorisation après sa première utilisation.
- Alice ne devrait pas avoir besoin d'intervenir manuellement dans la procédure d'autorisation OAuth (par exemple en entrant une adresse URL ou un mot de passe). (L'authentification d'Alice auprès de www.X-carrier.example ne relève pas du protocole OAuth.)

I.2 Cas d'utilisation: justificatif client

Description

L'entreprise Good-X-Pay établit les feuilles de paie des employés de l'entreprise Good-X-Work. Pour ce faire, l'application www.Good-X-Pay.example obtient un accès avec authentification aux données concernant la présence des employés stockées sur www.Good-X-Work.example. L'authentification est réalisée par le serveur d'autorisation, qui fait partie d'un réseau NGN avec l'URL www.X-carrier.example.

Conditions préalables

- L'application www.Good-X-Pay.example a défini, lors de l'enregistrement, un identificateur et un secret partagé avec le serveur d'autorisation www.X-carrier.example.
- Le type d'accès aux données stockées sur www.Good-X-Work.example dont bénéficie l'application www.Good-X-Pay.example a été défini.

Déroulement

Lorsque la procédure est menée à bien, l'application www.Good-X-Pay.example reçoit un jeton d'accès après s'être authentifiée auprès du serveur d'autorisation www.X-carrier.example. L'application www.Good-X-Pay.example utilise alors ce jeton pour accéder aux données concernant la présence stockées sur www.Good-X-Work.example.

Exigences

- L'authentification de l'application www.Good-X-Pay.example auprès du serveur d'autorisation www.X-carrier.example est obligatoire.
- La méthode d'authentification doit reposer sur un identificateur et un secret partagé, que l'application installée sur www.Good-X-Pay.example soumet au serveur d'autorisation www.X-carrier.example dans la demande HTTP initiale.
- Dans la mesure où la procédure permet d'accéder à des données sensibles appartenant à Good-X-Work, Good-X-Work doit établir une relation de confiance avec Good-X-Pay et le serveur d'autorisation www.X-carrier.example.

I.3 Cas d'utilisation: assertion

Description

L'entreprise Good-X-Pay établit les feuilles de paie des employés de l'entreprise Good-X-Work. Pour ce faire, l'application www.Good-X-Pay.example obtient un accès avec authentification aux données concernant la présence des employés stockées sur www.Good-X-Work.example. Le serveur www.Good-X-Work.example accorde un accès à l'application www.Good-X-Pay.example après avoir reçu un jeton d'accès délivré par le serveur d'autorisation www.X-carrier.example. Le serveur d'autorisation www.X-carrier.example authentifie l'application www.Good-X-Pay.example en validant une assertion que www.Good-X-Pay.example a présentée.

Ce cas d'utilisation décrit une solution différente de celle décrite dans le cas d'utilisation "justificatif client".

Conditions préalables

- L'application www.Good-X-Pay.example a obtenu une assertion d'authentification auprès d'une partie jouissant de la confiance du serveur d'autorisation www.X-carrier.example.
- Le type d'accès aux données stockées sur www.Good-X-Work.example dont bénéficie l'application www.Good-X-Pay.example a été défini.
- Le serveur d'autorisation www.X-carrier.example a établi une relation de confiance avec le producteur d'assertion et est capable de valider ses assertions.

Déroulement

Lorsque la procédure est menée à bien, l'application www.Good-X-Pay.example reçoit un jeton d'accès après s'être authentifié auprès du serveur d'autorisation www.X-carrier.example en présentant une assertion (par exemple, une assertion SAML). Il obtient l'accès aux données concernant la présence des employés en utilisant le jeton d'accès.

Exigences

- L'authentification de l'application www.Good-X-Pay.example auprès du serveur d'autorisation www.X-carrier.example est obligatoire.
- Le serveur d'autorisation www.X-carrier.example doit être capable de valider les assertions délivrées par le producteur d'assertions et présentées par l'application installée à l'adresse www.Good-X-Pay.example.
- Good-X-Work doit établir une relation de confiance avec Good-X-Pay et le serveur d'autorisation www.X-carrier.example.

Bibliographie

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[b-UIT-T X.1252] Recommendation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité*.

[b-UIT-T Y.2091] Recommandation UIT-T Y.2091 (2008), *Réseaux de prochaine génération: termes et définitions.*

[b-IETF RFC 6750] IETF RFC 6750, *The OAuth 2.0 Authorization Framework: Bearer Token Usage*.

[b-OpenID v.2] OpenID Authentication 2.0 <http://openid.net/specs/openid-authentication-2_0.html>

[b-3GPP TS 33.220] 3GPP TS 33.220 (2013) *Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture, Release 12*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2014